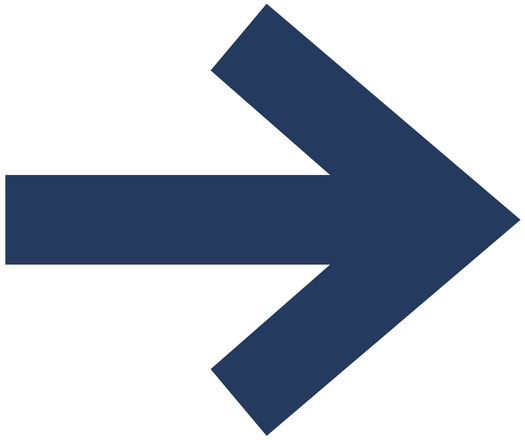
Windows 11

Comenzar por el punto de conexión

Un nuevo enfoque para la modernización de los dispositivos, los sistemas y el trabajo el equipo



El punto de conexión es el nuevo lugar de trabajo

Este eBook no le contará que el mundo ha cambiado, que los trabajadores desean tener mayor flexibilidad, que los clientes desean tener más comodidad, que los ciberdelincuentes quieren sus datos o que puede usar la tecnología para hacer frente a estos desafíos: los líderes empresariales y de TI ya saben todo eso.

Lo que puede ser menos conocido es el concepto de centrarse en los puntos de conexión, como PC y dispositivos móviles, como punto de partida para impulsar proyectos de modernización a gran escala. Tradicionalmente, para habilitar el trabajo remoto, implementar nuevas medidas de seguridad o simplificar la administración de TI, una organización debía implementar y administrar una solución independiente para cada objetivo. Además de tener que volver a implementar algunas soluciones varias veces para ejecutarlas en varios dispositivos.

Sin embargo, la generalización del trabajo remoto ha inspirado (o ha requerido, según el punto de vista) un nuevo enfoque en el que todas estas capacidades se incorporan en el sistema operativo en sí. Los posibles beneficios y retorno de la inversión (ROI) son importantes. Los empleados disfrutan de experiencias con menos complicaciones y más seguras, con menos tiempo de inactividad (incluso cuando trabajan en dispositivos personales) y los departamentos de TI pueden gobernar de mejor manera los dispositivos, la infraestructura y la seguridad desde una única herramienta de administración.

La modernización de los puntos de conexión es una forma práctica de obtener estos beneficios. Es una inversión fundamental que simplifica las operaciones, protege los datos y prepara a su organización para la resiliencia y el crecimiento.

Definición / modernización de puntos de conexión:

La práctica de mejorar la facilidad de uso, el rendimiento del hardware y software, la funcionalidad cruzada y la seguridad de los equipos de escritorio, tabletas y dispositivos móviles de los trabajadores. Esto incluye los dispositivos personales que ejecutan aplicaciones para trabajar.

Capítulo

/ 01

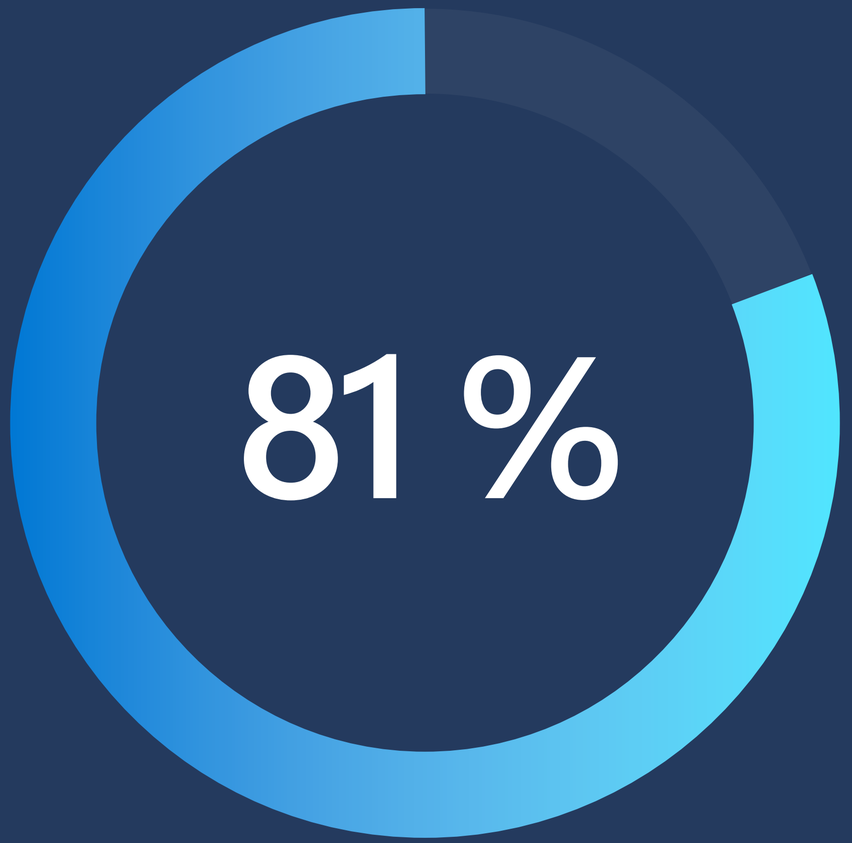
Aumente la flexibilidad mediante la modernización de los puntos de conexión

Trabajar en cualquier momento y lugar, desde cualquier dispositivo, solía ser una ventaja. En la actualidad, es fundamental para la mayoría de las personas y empresas.[1] De hecho, en un estudio de Forrester encargado por Microsoft, los empleados manifestaron que, al permitir que las personas usen sus dispositivos personales para trabajar, así como para trabajar con mayor flexibilidad entre el hogar y la oficina, mejora la satisfacción de los empleados y se reduce la rotación de personal.[2]

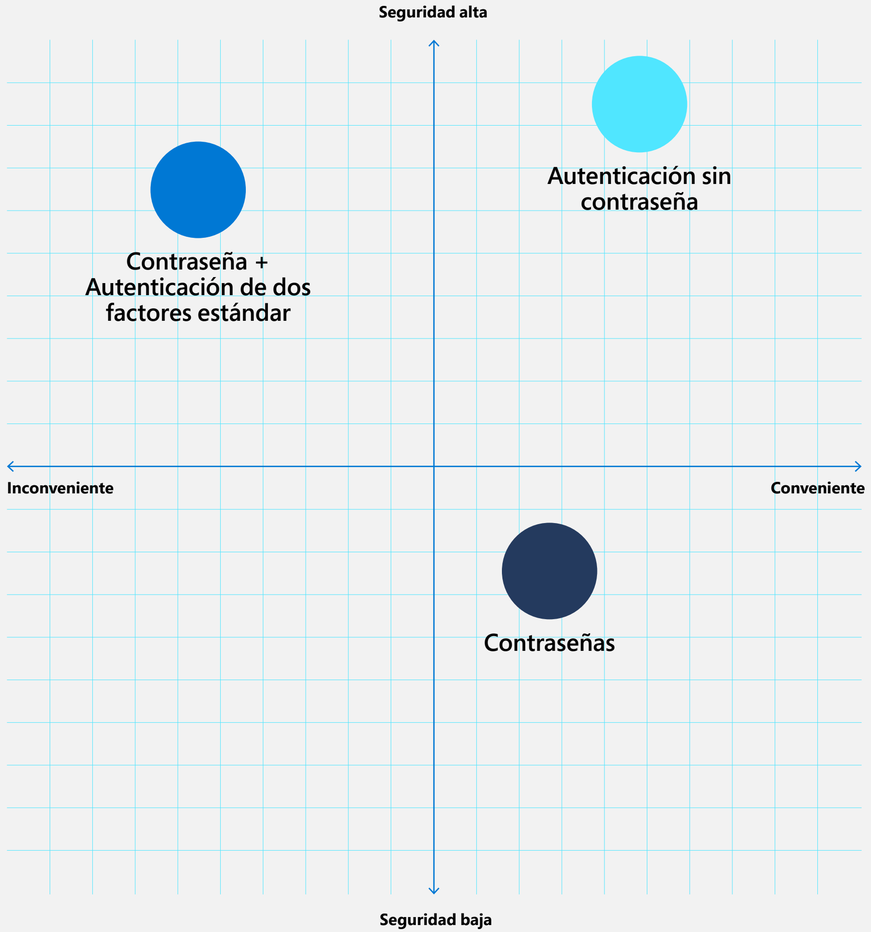
Hacer el cambio entre dispositivos no solo debe ser posible, debe ser fácil y tener un aspecto coherente. Las personas deben ser capaces de crear una presentación en su equipo portátil, editarla en su teléfono y presentarla con su tableta, todo sin tener que solucionar problemas de sus dispositivos. La experiencia completa debe ser intuitiva y no presentar problemas, para que así las personas puedan mantener el flujo de trabajo. Para cumplir con estos requisitos, los departamentos de TI se centran cada vez más en el sistema operativo de los puntos de conexión de los empleados como estrategia de modernización clave.

[1] "The winner by a long stretch", The WorkLab Year in Review, Microsoft, 2021.
[2] The Total Economic Impact™ Of Modernizing Endpoints, estudio de Forrester Consulting encargado por Microsoft, septiembre de 2021.

Porcentaje de líderes empresariales que ajustan sus directivas de flexibilidad en el lugar de trabajo



La autenticación sin contraseña es más segura y conveniente que otras opciones



La flexibilidad comienza en TI

La entrega de flexibilidad a los empleados comienza en el departamento de TI, al equipar a los trabajadores de TI y seguridad con las herramientas que necesitan para ahorrar en presupuesto y brindar soporte remoto a los puntos de conexión.

Para que esto sea posible sin que se requiera un compromiso de tiempo importante, los líderes de TI deben considerar la implementación de soluciones como aplicaciones de administración de puntos de conexión que admitan la administración de dispositivos locales y en la nube.

Otra manera de ofrecer flexibilidad es mediante el cambio a la autenticación sin contraseña. Windows 11 está diseñado específicamente para optimizar este proceso y simplificar la implementación, de modo que las personas puedan iniciar sesión con solo una pulsación o una mirada. Es más rápido y fácil para los empleados, y mucho más difícil de hackear. Además, la implementación de la autenticación multifactor, una parte clave de la autenticación sin contraseña, puede frustrar el 99,9 % de los ciberataques.[3]

La modernización de los sistemas operativos es clave

Brindar a los empleados mayor flexibilidad no necesariamente significa proporcionarles lo último en teléfonos o equipos portátiles. Se trata de adoptar una estrategia de TI que permita a las personas usar el dispositivo de su elección, con seguridad integrada. Para implementar esa estrategia en amplios sectores y lograr sus objetivos de flexibilidad, considere actualizar su sistema operativo y, según sea necesario, los dispositivos de punto de conexión que no sean compatibles con versiones más recientes de los sistemas operativos.

[3]Passwordless Protection: Reduce your risk exposure with passwordless authentication, Microsoft Security, 2021.

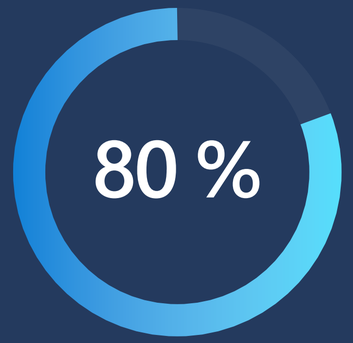
Capítulo

/ 02

Ofrezca experiencias sorprendentes a los empleados

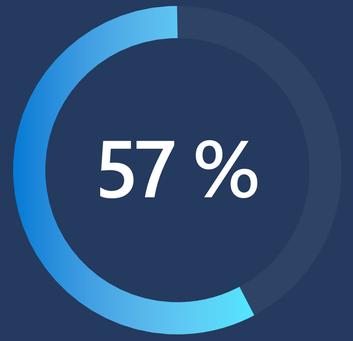
De acuerdo con el Índice de tendencias laborales de Microsoft 2022, 80 % de los empleados señaló que, desde que adoptaron la modalidad híbrida, su productividad se mantuvo o mejoró. El 57 % de los empleados remotos está considerando cambiar al trabajo híbrido, mientras que el 51 % de los empleados híbridos está considerando cambiar al trabajo remoto. Además, los trabajos remotos en LinkedIn atraen 2,6 veces más vistas y casi 3 veces más aplicantes en comparación con los roles in situ.[4] Las empresas que ofrecen esta flexibilidad con un entorno de punto de conexión modernizado se destacarán en un mercado competitivo de talentos.

Para tener éxito, todo el mundo, incluidos los trabajadores de primera línea, los ejecutivos y los trabajadores de la información, necesita colaborar sin problemas, tener acceso rápido a la información y aprovechar el tiempo de concentración en el trabajo y su propio bienestar. Además, los empleados que pueden completar fácilmente sus tareas, sin importar dónde estén, son más felices y más productivos.[5] Un entorno modernizado de puntos de conexión les ayuda a mantener el control de su día y da forma a las percepciones que tienen de su organización.

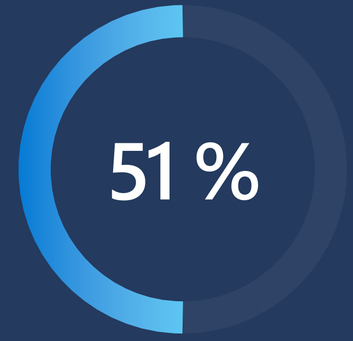


de los empleados señala que su productividad se mantuvo o mejoró con la modalidad híbrida

más aplicantes para trabajos remotos que in situ



de los empleados remotos están considerando cambiar al trabajo híbrido



de los empleados híbridos están considerando cambiar al trabajo remoto

[4]2022 Work Trend Index: Annual Report: Great Expectations: Making Hybrid Work *Work*, Microsoft, 16 de marzo de 2022.
[5]The Total Economic Impact™ Of Modernizing Endpoints, estudio de Forrester Consulting encargado por Microsoft, septiembre de 2021.

Cree un lugar de trabajo próspero

Mejorar las experiencias de los empleados con sus dispositivos no solo significa ayudarlos a trabajar más rápido, sino también empoderarlos para que contribuyan a la empresa de forma más significativa. De acuerdo con un informe de Forbes Insights, "Los empleados se benefician de una experiencia sencilla y uniforme que mejora su eficiencia, colaboración y comunicación con los clientes y entre sí".[6]

La clave para esto es eliminar la fricción de alternar entre puntos de conexión para que los empleados no tengan que desviar el foco de su trabajo para comenzar a usar otro dispositivo. Por ejemplo, un sistema operativo que ofrece contenido seleccionado puede ayudarlos a planificar su día y a tener acceso fácil a personas y archivos, sin importar el dispositivo que usen. Los métodos sin contraseña, como el escaneo de huellas dactilares, los PIN y el reconocimiento facial, optimizan el registro y el inicio de sesión en las aplicaciones. Además, la escritura por voz y la compatibilidad con gestos y lápices ópticos facilitan el trabajo en cualquier dispositivo.

Cree una cultura inclusiva

Los departamentos de TI pueden ayudar a fomentar una cultura positiva y próspera en los equipos híbridos mediante la implementación de tecnología que respalde la participación de las personas con diferentes estilos de comunicación y experiencias. Un entorno de puntos de conexión unificado fomenta la colaboración entre dispositivos, ubicaciones y documentos. La adopción de herramientas que usan principios de diseño intuitivos facilitan la iniciación y la participación en reuniones y conversaciones con personas dentro de la oficina y en todo el mundo.

Un lugar de trabajo inclusivo que permite a los empleados ser ellos mismos y hacer cosas es un potente diferenciador para las organizaciones empresariales. La modernización de los puntos de conexión le ayudará a ofrecer una experiencia digital que hará que su lugar de trabajo sea más productivo y divertido.

[6]"Section IV: Endpoint Modernization," Reimagining Endpoints: Productive and Secure Computing in Today's Hybrid, Front-Line and Edge Environments, Forbes Insights en asociación con Microsoft, 2021.

Capítulo

/ 03

Proteja a las personas, los datos y los servicios

A medida que los empleados amplían la cantidad y la variedad de dispositivos que usan para hacer su trabajo, incluidos sus dispositivos personales, los departamentos de TI realizan un gran trabajo para mantener los puntos de conexión en regla y actualizados. Un estudio de líderes de TI empresariales reveló algunos desafíos comunes[7]:

- Soluciones de seguridad unidas que son dispares y están obsoletas.
- Dependencia excesiva de las VPN, administración de identidades obsoleta y controles de administración de dispositivos inadecuados.
- Mayor riesgo de filtración de datos, directivas de autenticación restrictivas que degradan la experiencia del empleado y obstáculos para incorporar nueva tecnología y a nuevos empleados.

Para abordar estos desafíos, las organizaciones están adoptando cada vez más la **arquitectura de Confianza Cero** como un enfoque integral que protege los entornos donde puede llevar su propio dispositivo, los recursos basados en la nube y a los usuarios remotos.[8]

La seguridad del punto de conexión comienza con un enfoque integral de Confianza Cero

Los principios de la Confianza Cero son:

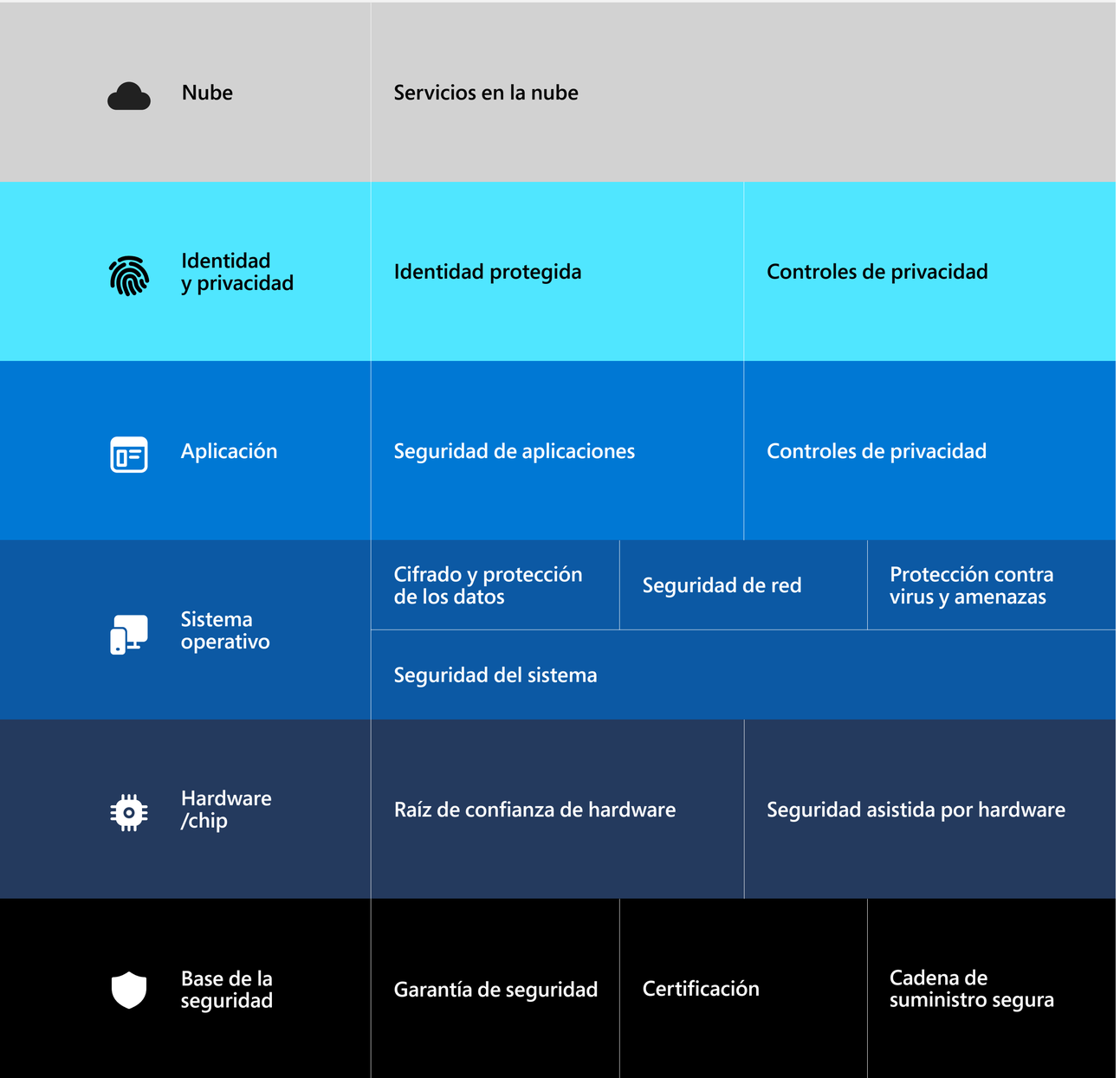
1. **Verificar explícitamente**. Autentique y autorice siempre en función de todos los puntos de datos disponibles.
2. **Usar el acceso con menos privilegios**. Limite el acceso de los usuarios con el acceso just-in-time y just-enough (JIT/JEA), directivas de adaptación basadas en riesgos y protección de datos.
3. **Suponer la vulneración**. Minimice el radio de explosión y el acceso a los segmentos. Verifique el cifrado de extremo a extremo y utilice análisis para mejorar la visibilidad, la detección de amenazas y las defensas.

Microsoft fomenta el uso de controles de Confianza Cero para proporcionar visibilidad, automatización y organización en las identidades, los puntos de conexión, las aplicaciones, la infraestructura de red y los datos.

Confianza Cero en el patrimonio digital

[7]The Total Economic Impact™ of Zero Trust Solutions from Microsoft: Cost Savings and Business Benefits Enabled by Microsoft's Zero Trust Solutions. Un estudio encargado realizado por Forrester Consulting en nombre de Microsoft. Diciembre de 2021.
[8]McKendrick, Joe. Reimagining Endpoints: Productive and Secure Computing in Today's Hybrid, Frontline, and Edge Environments. ©Forbes Insights 2021.

Las seis capas de la seguridad de Confianza Cero



La Confianza Cero se extiende desde el chip hasta la nube

Las estrategias sólidas de seguridad de extremo a extremo deben:

- **Separar el hardware del software** para la protección contra amenazas: el dispositivo de punto de conexión se protege incluso antes de que se inicie.
- **Proteger el sistema operativo** contra el acceso no autorizado a los datos críticos.
- **Priorizar la seguridad** de las aplicaciones e impedir el acceso a código no verificado.
- **Proteger las identidades de los usuarios** con seguridad sin contraseña.
- **Extender la seguridad a la nube,** para así proteger los dispositivos, los datos, las aplicaciones y las identidades de forma remota.

La seguridad de Confianza Cero en el punto de conexión comienza con el aislamiento basado en hardware en el nivel de chip. Los datos confidenciales se almacenan tras barreras de seguridad y se mantienen separados del sistema operativo, por lo que las claves de cifrado y las credenciales de usuario quedan protegidas ante el acceso no autorizado.

Las organizaciones deben implementar características de seguridad para el hardware y los sistemas operativos que:

- **Protejan y mantengan la integridad del sistema** a medida que se carga el firmware, lo que impide que el firmware o software se inicie antes de que se inicie el sistema operativo.
- **Usen un módulo de plataforma confiable** (TPM) 2.0 para características como Windows Hello y BitLocker.
- **Creen seguridad basada en la virtualización** mediante la virtualización del hardware de la CPU para proteger una región de memoria aislada del sistema operativo para proteger la información y la integridad del código.

Un desarrollo interesante en la tecnología de raíz de confianza de hardware es Pluton, un procesador de seguridad diseñado por Microsoft para impedir ataques sofisticados. El chip se puede configurar como el TPM del dispositivo o como procesador de seguridad en escenarios que no son de TMP, como la resiliencia de la plataforma.


Chart
Sales Goal
67%
Junk
Yesterday
Wanda Howard
Tomorrow's Sync
12:55 PM
Let's make sure that we come prepared to
Elvia Atikins
Team Pictures
12:55 PM
We look forward to meeting our fall intervi
Tomorrow, 11:00 AM (30m
RSVP
Alpine Ski House
Opportunity
South Africa Coffee
Opportunity
People
Aadi Kapoor
Files
Trade financing proposal
South African deck
Aida Proposal estimates
12:40
Microsoft

Capítulo

/ 04

Mitigue los riesgos y vulnerabilidades

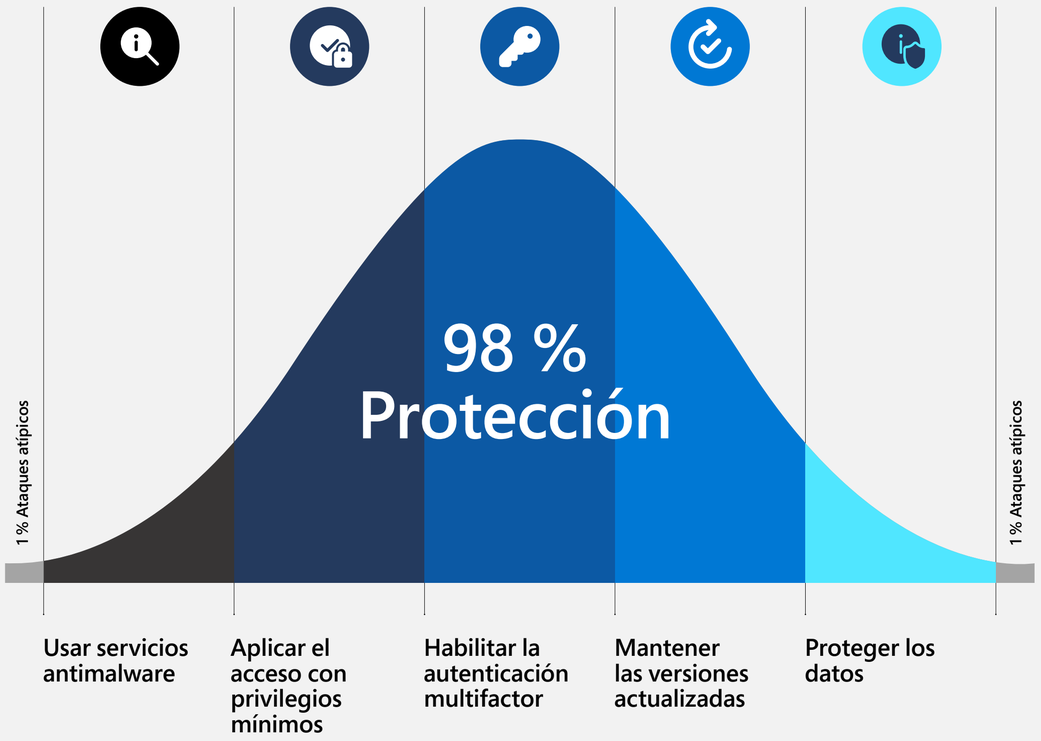
La percepción común es que los ciberataques son operaciones complejas y difíciles de detener. Pero la realidad es que la negación o resistencia de los empleados a seguir procedimientos de seguridad básicos recomendados, para la creación de contraseñas y la identificación de intentos de suplantación de identidad (phishing). De hecho, las contraseñas robadas son, por mucho, la manera más común en la que se vulneran las cuentas y los datos de las empresas. Incluso los ataques de agentes de estados-nación se basan en tácticas simples como difusión de contraseñas, que capitalizan a los empleados que usan contraseñas débiles.[9]

Solo en 2021, Microsoft detectó y bloqueó más de 25 mil millones de intentos de secuestrar cuentas empresariales.[10] Estos no eran ataques sofisticados. Eran simples intentos de inicio de sesión de fuerza bruta y contraseñas robadas.

Entonces, ¿por qué tantos departamentos de TI tienen problemas para impedir estas vulneraciones? La explicación es simple: es más un problema de personas que un problema de tecnología. Por lo tanto, si bien los departamentos de TI deben seguir instruyendo a los empleados en procedimientos básicos de seguridad, existen dos soluciones de modernización de puntos de conexión que ayudan a mitigar la parte del problema que implica al "personal" y, por ende, la gran mayoría de los ataques: la autenticación multifactor y la aplicación de parches.

[9] "Identity is the New Battleground," Cyber Signals, diciembre – enero de 2021.
[10] Ibid.

La curva de la ciberseguridad: la higiene básica sigue protegiendo contra el 98 % de los ataques



Menos del 20 % de los clientes de Microsoft emplean la autenticación multifactor.[11]

[11]Informe de defensa digital de Microsoft, octubre de 2021.

Aspectos esenciales de la higiene de seguridad básica

- **Un enfoque de Confianza Cero** para la autenticación. Confianza Cero supone que la seguridad de su sistema operativo ya ha sido vulnerada y requiere que los empleados verifiquen constantemente sus identidades mediante la autenticación multifactor.
- **Autenticación multifactor.** Los empleados proporcionan múltiples formas de identificación, tales como un token de hardware y biometría, para acceder a sus cuentas y datos.
- **La autenticación sin contraseña** elimina la necesidad de contraseñas generadas por los empleados, que suelen ser el eslabón más débil de la seguridad de una organización.
- **La actualización y aplicación de parches al software** es una forma sencilla, pero eficaz, de prevenir los ataques. Los departamentos de TI deben implementar actualizaciones automáticas para reforzar la seguridad en toda la organización.

Protección contra amenazas avanzada

Junto con la higiene de seguridad básica, la implementación de protección contra amenazas avanzada que detecta y responde a los ataques antes de que estos puedan causar daño es fundamental. Las organizaciones deben usar:

- **Un firewall de host,** como Windows Defender Firewall, para limitar los dispositivos que pueden entrar a la red y los datos que se pueden enviar desde dentro, así como para exigir la autenticación de cualquier dispositivo que intente comunicarse con los dispositivos de la red.
- **Software antivirus multifacético** que unifique machine learning, el análisis de macrodatos y la investigación de resiliencia en profundidad para proporcionar protección completa a los dispositivos del punto de conexión. Un ejemplo reconocido es Microsoft Defender Antivirus.

Capítulo

/ 05

Permita la administración unificada

Una ventaja clave de la modernización de los puntos de conexión es la oportunidad de, simultáneamente, unificar las herramientas de administración de TI, ahorrarle tiempo al equipo de TI y minimizar los costos de administración. Además de impulsar la eficiencia, el uso de un único centro de control para administrar los puntos de conexión de su organización aumenta la velocidad, la escala y la coherencia de los esfuerzos de seguridad de red.

Contar con un panel de control administrativo unificado que está incorporado en el sistema operativo, como Windows 11, le permite:

- Administrar los dispositivos de punto de conexión, la seguridad y los recursos en la nube desde un solo lugar.
- Proteger, implementar y administrar los dispositivos corporativos y personales sin interrumpir el trabajo.
- Simplificar la TI con herramientas que permiten que diferentes proveedores y soluciones trabajen juntos.
- Implementar más fácilmente las actualizaciones de seguridad, los parches y las directivas en toda su organización.
- Evaluar rápidamente el cumplimiento de los PC y dispositivos individuales o de toda la empresa.
- Proteger con mayor eficacia contra las vulneraciones de datos mediante el cifrado de todos los datos en el sistema.

Administración de seguridad avanzada

Aquí daremos un vistazo más de cerca a dos características de administración de seguridad unificada de las que las organizaciones que ejecutan Windows deben hacer uso completo: **administración avanzada de directivas de grupo** y **administración moderna de la administración de BitLocker**.

Administración avanzada de directivas de grupo

El uso de la administración avanzada de directivas de grupo para mantener actualizadas sus configuraciones de usuario y de escritorio le permite a los administradores de su red trabajar más rápido y a mayor escala. Además, ayuda a reducir el tiempo de inactividad para los empleados en toda su organización.

En lugar de tener que configurar uno a uno cada equipo en un entorno de Windows Server Active Directory, puede usar una consola central para configurar todos los sitios, dominios y unidades organizativas. Además de reducir el costo total de propiedad, esto le da al equipo de TI un control más granular sobre las actualizaciones claves del punto de conexión.

Administración moderna de la administración de BitLocker

El uso de la administración moderna de la administración de BitLocker optimiza la implementación y la supervisión de los dispositivos protegidos con BitLocker, y le permite proteger los puntos de conexión con mayor eficiencia contra la pérdida y el robo de datos.

Esto permite al equipo de TI automatizar el cifrado de volúmenes en los equipos cliente de toda la organización, supervisión del cumplimiento y la elaboración de informes, y simplificar la recuperación de claves. También permite a los empleados aprovechar las herramientas de autoservicio para recuperar los dispositivos cifrados por sí mismos, sin que deban ponerse en contacto con el soporte técnico. Todo esto ayuda a escalar la implementación de dispositivos y a reducir el costo de aprovisionamiento y soporte de unidades cifradas.

Capítulo

/ 06

Aumente la productividad de TI

Los equipos de TI observan dos tipos de beneficios empresariales que se obtienen de la modernización del punto de conexión: **simplificación o automatización de las tareas repetitivas** y **consolidación o eliminación de soluciones redundantes**.

Simplificación o automatización de las tareas repetitivas

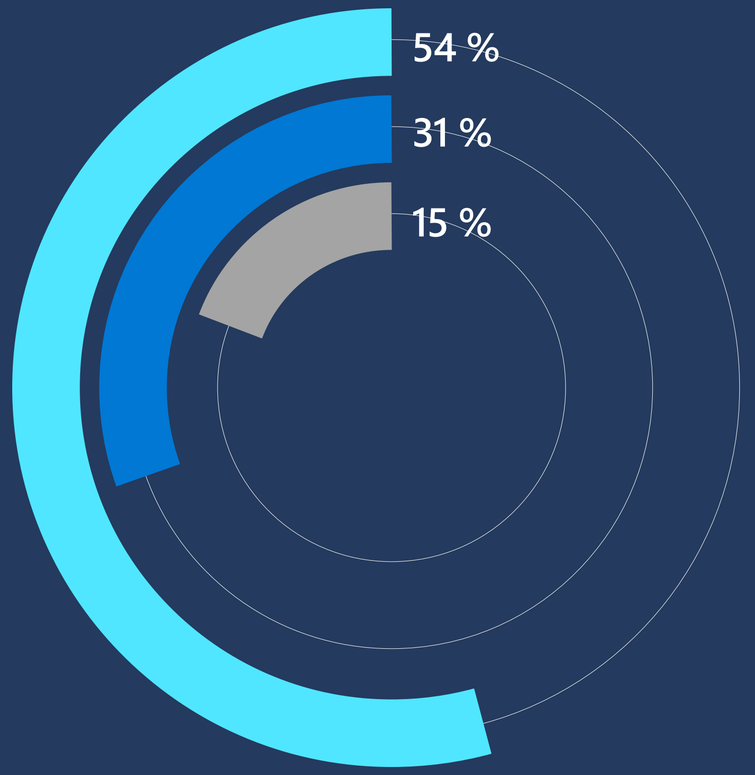
Sabemos que los sistemas operativos modernizados proporcionan a los usuarios de puntos de conexión experiencias con menos complicaciones, mayor seguridad y flexibilidad, y mitigación de riesgos integrada. Pero para los equipos de TI que administran la tecnología del punto de conexión, estos beneficios también se traducen en una mayor productividad. El tiempo que anteriormente dedicaban a hacer tareas repetitivas y cotidianas se liberó para el trabajo de mayor valor. Esto es especialmente beneficioso para los departamentos de TI con personal y recursos limitados.

Las posibles ganancias en términos de eficiencia incluyen:

- **Menos llamadas a soporte.** Mediante el uso de herramientas como el PIN de BitLocker o un portal de autoservicio, los usuarios del punto de conexión pueden resolver más problemas tecnológicos por sí solos. Cuando los propios empleados se hacen cargo de tareas como la actualización de aplicaciones o las credenciales de inicio de sesión, el personal de soporte recupera tiempo para dedicarlo a otros proyectos.
- **Implementación de soluciones y actualizaciones a escala.** La mayoría de los equipos de TI aún proporcionan y actualizan dispositivos de punto de conexión in situ.[12] Los puntos de conexión modernizados permiten realizar la implementación fácilmente con las capacidades de implementación remota y automatizada.
- **Administración de directivas globales.** Los sistemas de administración de puntos de conexión modernizados permiten a los equipos de TI administrar la mayoría de las tareas (como el cumplimiento y la seguridad) desde un único centro de control. Las directivas administradas centralmente hacen que sea más fácil mantener actualizadas las configuraciones de escritorio de toda la empresa y reducen el tiempo de inactividad de los empleados.

[12]The Total Economic Impact™ Of Modernizing Endpoints, estudio de Forrester Consulting encargado por Microsoft, septiembre de 2021.
[13]Ibid.

La mayoría de los departamentos de TI de la empresa aprovisionan, actualizan y protegen los puntos de conexión in situ



Base: 301 global IT decision-makers
Fuente: Un estudio encargado realizado por Forrester Consulting en nombre de Microsoft, marzo de 2021.[13]

Solo quiero comprar una licencia para las cosas. No quiero comprar dos licencias para la misma capacidad.[14]

—Director de servicios para los usuarios y operaciones de seguridad de una organización farmacéutica

Consolidación o eliminación de soluciones redundantes

Los puntos de conexión modernizados también ofrecen a los equipos de TI la oportunidad de consolidar (o incluso eliminar) servicios y soluciones dispares o redundantes. Esto libera presupuesto, tiempo y recursos para otros proyectos.

Las soluciones de software dispares incurren en gastos cuantificados y no cuantificados. **Los gastos cuantificados** son los costos que se miden con una cifra monetaria, como los acuerdos de costo de licencias y los costos de soporte de proveedores. **Los gastos no cuantificados** incluyen las inversiones más difíciles de medir, como el tiempo y el esfuerzo de un empleado para aprender a operar una nueva solución de software e implementarla dentro de un ecosistema de software existente.

Los puntos de conexión modernizados no solo tienen el software más reciente, sino también una gran cantidad de soluciones integradas que están incorporadas en el sistema operativo. Con un conjunto de soluciones diseñadas para trabajar juntas desde el principio, los equipos de TI pueden desechar los servicios redundantes y liberar tiempo y recursos que anteriormente dedicaban al mantenimiento de soluciones. Desde el punto de vista de la optimización de costos, abundan las oportunidades. En el estudio Total Economic Impact™ Of Modernizing Endpoints de Forrester Consulting encargado por Microsoft se calcula que la eliminación de soluciones de software redundante tiene como resultado una reducción de costos de más de USD 607.000 en un período de tres años para una organización compuesta por 4.000 personas.[15]

[14]Ibid.
[15]Ibid.

Evalúe y desarrolle la estrategia de puntos de conexión de su organización

Puede que le sorprenda que un eBook que recomienda la modernización de los puntos de conexión también recomiende a algunas empresas mantener sus estrategias actuales de punto de conexión. Lo cierto es que muchas organizaciones han habilitado con éxito el trabajo remoto, mejorado sus herramientas de colaboración en el lugar de trabajo, implementado medidas de seguridad avanzadas y unificado su administración de TI mediante la implementación de soluciones complementarias independientes. Después de todo, Microsoft ha ayudado a las organizaciones a hacer esto durante mucho tiempo.

Pero la realidad es que ahora tiene más sentido para Windows tratar los dispositivos de trabajo y personales, las herramientas del lugar de trabajo, los recursos en la nube y la seguridad como si fueran interoperables de forma predeterminada, porque para la mayoría de los empleados y departamentos de TI, ahora lo son. Y aunque Windows 10 seguirá siendo una plataforma de innovación para muchas organizaciones exitosas, Windows 11, que se puede implementar en el mismo entorno que Windows 10, está específicamente diseñado para satisfacer esas necesidades de manera más integral.

Dondequiera que se encuentre en sus planes de modernización de puntos de conexión, esperamos que la orientación de este eBook le proporcione un marco útil para evaluar y desarrollar la estrategia de punto de conexión de su organización.

Más información sobre Windows 11
O explore la documentación de implementación